Missouri Law Review

Volume 82
Issue 2 *Spring 2017*

Article 9

Spring 2017

It's Probable: Missouri Constitution Article I, Section 15 Requires a Higher Standard to Obtain a Warrant for Real-Time or Prospective CSLI

Aaron Hadlow

NOTE

It's Probable: Missouri Constitution Article I, Section 15 Requires a Higher Standard to Obtain a Warrant for Real-Time or Prospective CSLI

Aaron Hadlow[*]

I. INTRODUCTION

There are more active cell phones in the United States than there are people.[1] Law enforcement officers often use electronic communication data during criminal investigations to surveil suspects.[2] Law enforcement officers

---

[*] B.A., Philosophy, Missouri State University, 2011; J.D. Candidate, University of Missouri School of Law, 2018. I would like to extend my gratitude to Professor Bowman, whose early guidance and valuable ongoing feedback as faculty advisor steered this Note in a more favorable direction; the editorial board members of the *Missouri Law Review*, who I am humbled to associate with as colleagues, and whose suggestions unquestionably improved this Note in ways I could not on my own. I extend particular thanks to Bradley Craigmyle, Ben Levin, Jack Downing, Tom Wright, Emily Mace, and the many *Law Review* members whose labors in footnote checking are greatly appreciated. I thank my family for their continued support, especially my wife Rebekah, whose love is given without hesitation and whose confidence I share in every endeavor.

1. According to an annual survey conducted by the CTIA, an organization representing the wireless communications industry, wireless subscribers equaled 115.7% of the U.S. population. *Annual Wireless Industry Survey*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last updated Oct. 2016) [hereinafter CTIA Survey]. In December 2015, there were an estimated 377.9 million wireless subscriber connections. *Id.*

2. In 2015, the U.S. district courts in Missouri authorized fifty-six wiretap applications, primarily for monitoring the content of electronic communication data on cell phones. OFFICE OF ADMIN., WIRETAP REPORT 2015 tbl.2 (Dec. 31, 2015), http://www.uscourts.gov/sites/default/files/data_tables/wiretap_2_1231.2015.pdf [hereinafter WIRETAP REPORT 2015]. These applications, however, only incorporate those applications by law enforcement made under the Wire and Electronic Communications Interception and Interception of Oral Communications Statute. *Id.*; 18 U.S.C. §§ 2510–2522 (2012). They do not incorporate applications for CSLI under The Stored Communication Act. *Id.* §§ 2703–2712. Applications granted under § 2703 are included in a separate report for delayed-notice search warrants. *Id.* § 2703. Data reported for § 2703 applications are only available through 2014, when the U.S. district courts in Missouri authorized 191 delay-notice search warrants. OFFICE OF ADMIN., DELAYED-NOTICE SEARCH WARRANT REPORT 2014 tbl.2 (Dec. 31, 2014), http://www.uscourts.gov/sites/default/files/table_2_0.pdf.

are able to do so because cell phone ownership is nearly universal.[3] Cell phones emit signals to the nearest cell phone tower every seven seconds.[4] Once the signal is received by the cell tower, it is recorded in signal logs, which are stored by cell service providers.[5] This information is called "cell-site location information" ("CSLI").[6] Under federal statute, law enforcement may access these records as both historic data and as real-time CSLI.[7] Historic CSLI is a record retained by the cell service provider of the cell phone's signal transmissions to cell towers.[8] Real-time CSLI is the data "stream[ed] continuously" by a cell phone to a cell tower.[9] In most cases, an authorized governmental authority can access this information without knowledge of the phone's user.[10]

The scope of this Note primarily deals with issues surrounding real-time CSLI, although the issues implicated by article I, section 15 of the Missouri Constitution could apply to historic CSLI as well. Part II of this Note discusses general principles of Fourth Amendment law and the Supreme Court's treatment of searches and seizures in relation to electronic communications and data. It then discusses the statutory developments empowering law enforcement to use emerging technologies for surveillance purposes. Part III discusses recent developments in search and seizure law. It then discusses Missouri's recent amendment to its constitution, which provides additional protections for electronic communications and data. Part IV discusses the impact of recent legal developments on CSLI and law enforcement practice.

---

3. There are an estimated 8.1 billion devices connected wirelessly worldwide. *See Over 8 Billion Connected Devices Globally, IHS Says*, IHS MARKIT (June 10, 2016, 6:40 AM), http://news.ihsmarkit.com/press-release/technology/over-8-billion-connected-devices-globally-ihs-says. On average, there are four wireless devices per household across the globe. *See id.*

4. Alison Healey, *Answering the Call: The Latest News on Tracking Individuals via Their Cellular Phones*, FED. L. ENFORCEMENT TRAINING CTRS. 1, https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/TrackingIndividualsviaTheirCellularPhones.pdf (last visited Mar. 26, 2017). There are more than 307,000 cell tower sites located in the United States. CTIA Survey, *supra* note 1.

5. Healey, *supra* note 4.

6. *Id.*

7. *Id.*

8. 1 JAMES G. CARR, PATRICIA L. BELLIA & EVAN A. CREUTZ, LAW OF ELECTRONIC SURVEILLANCE § 4:88 (Aug. 2016).

9. *Id.* Some courts have held that only five minutes need to pass to change real-time CSLI to historic. *See* State v. Perry, 776 S.E.2d 528, 535 (N.C. Ct. App. 2015).

10. Under 18 U.S.C. § 2703, a delayed-notice warrant is often issued. Delay-noticed periods may be extended in practice indefinitely. 18 U.S.C. § 2705 (2012).

II. LEGAL BACKGROUND

Part II is broken into three parts. Part A reviews the general principles of Fourth Amendment law. Part B discusses the Supreme Court's development of surveillance law under the Fourth Amendment. Part C sketches the development of the modern surveillance statutory scheme under which Missouri law enforcement operates.

A. Fourth Amendment General Principles

The Fourth Amendment has two clauses. The first clause (the search and seizure clause) reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[11] The second clause (the warrants clause) reads: "*and no Warrants shall issue*, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[12] A seizure is "some meaningful interference

---

11. U.S. CONST. amend. IV.

12. *Id.* (emphasis added). James Madison's originally proposed amendment during the 1787 Constitutional Convention in Philadelphia seemed to intend that these two provisions be conjunctive, so that a reasonable search and seizure was necessarily conditioned upon the fulfillment of hard warrant requirements. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (5th ed. 2016). Madison's proposal read:

> The rights of the people to be secured in their persons, their houses, their papers, and their other property, from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.

Id. (quoting 1 ANNALS OF CONG. 452 (1789)). Madison's inclusion of the phrase "shall not be violated by warrants issued without" would appear to authorize all "unreasonable searches" if accompanied by any warrant, regardless of whether it was issued with probable cause, or the other warrant requirements. This was surely the opposite of what Madison intended. A more logical reading of Madison's proposal given the historical context is that Madison intended hard warrant requirements for all searches and seizures. These hard warrant requirements were even maintained through committee alterations. *Id.* However, the committee chairman reported the eventually adopted Fourth Amendment language, despite a majority of the committee voting against it, which includes the above-emphasized "and No warrants" language, which has been interpreted as separating the unreasonable search and seizure provision from the warrant requirement provision. *Id.* The "and No warrants" wording was included, over Constitutional Convention committee objection, to clarify the more dangerous ambiguity that existed on the face of Madison's original proposal. *Id.*

with an individual's possessory interests in that property."[13] A search within the meaning of the Fourth Amendment has never been explicitly defined by the Supreme Court of the United States.[14] However, law enforcement's access of CSLI has for many years been treated as a search.[15] Prior to 1967, the Supreme Court generally held that, in order for a search to occur, within the meaning of the Fourth Amendment, there had to be some physical intrusion into a "constitutionally protected area."[16] Constitutionally protected areas were limited to those enumerated in the text of the Fourth Amendment.[17] This was known as the trespassory doctrine.[18] In 1967, the Supreme Court turned away from this approach in *Katz v. United States*.[19]

In *Katz*, Charles Katz was convicted of transmitting wagering information by telephone across state lines in violation of federal gambling laws.[20] During trial, recordings of Katz's phone conversations were admitted into evidence.[21] The evidence was obtained after FBI agents had attached an "electronic listening and recording device" to the outside of the public telephone booth that Katz used to place the incriminating phone calls.[22] The Supreme Court was called on to determine whether the evidence was obtained in violation of the Fourth Amendment and therefore erroneously ad-

13. United States v. Jacobsen, 466 U.S. 109, 113 (1984). *Black's* defines a seizure as "[t]he act or an instance of taking possession of a person or property by legal right or process." *Seizure*, BLACK'S LAW DICTIONARY (10th ed. 2014).

14. 1 LAFAVE, *supra* note 12, § 2.1(a) ("The Supreme Court, quite understandably, has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment."). LaFave offers a traditional definition that has been used by several appellate courts. "Search" is said to imply:

> some exploratory investigation, or an invasion and quest, a looking for or seeking out. The quest may be secret, intrusive, or accomplished by force, and it has been held that a search implies some sort of force, either actual or constructive, much or little. A search implies a prying into hidden places for that which is concealed and that the object searched for has been hidden or intentionally put out of the way. While it has been said that ordinarily searching is a function of sight, it is generally held that the mere looking at that which is open to view is not a "search."

Id. § 2.1 (quoting 79 C.J.S. *Searches and Seizures* § 1 (1952)).

15. *See* United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015), *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016).

16. Silverman v. United States, 365 U.S. 505, 512 (1961).

17. These enumerations included "'persons,' including the bodies and clothing of individuals; 'houses,' including apartments, hotel rooms, garages, business offices, stores, and warehouse; 'papers,' such as letters; and 'effects,' such as automobiles." 1 LAFAVE, *supra* note 12, § 2.1(a) (footnotes omitted).

18. United States v. Jones, 132 S. Ct. 945, 949 (2012).

19. Katz v. United States, 389 U.S. 347 (1967).

20. *Id.* at 348.

21. *Id.*

22. *Id.*

mitted into evidence.[23] The Court dismissed the State's argument that the search was permissible under the Fourth Amendment because there was no physical trespass.[24] Instead, the Court ruled that "the Fourth Amendment protects people, not places."[25]

In *Katz*, Justice Harlan articulated in a concurrence the two-part test now known as the *Katz* test: "[F]irst[,] that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[26] The *Katz* ruling required law enforcement to obtain a warrant under the probable cause standard in order to conduct similar surveillance activities in the future.[27]

While *Katz* was a turning point in Fourth Amendment search doctrine, Supreme Court case law relating to the warrant clause of the Fourth Amendment has followed its own line of development. Given the practical realities of the work of law enforcement, a number of exceptions to the warrant requirement have been carved out over the years.[28] However, courts always prefer that police officers obtain a warrant before a search.[29] Federal Rule of Criminal Procedure 41, which most surveillance statutes refer to for warrant requirements, generally tracks the language of the Fourth Amendment, requiring the warrant to (1) describe the identity of the person or property to be searched or seized, (2) be issued by a magistrate judge or a judge of a state court of record, and (3) be served within a specified time period no longer than fourteen days after issuance.[30]

If some governmental act is deemed a search within the meaning of the Fourth Amendment, then regardless of whether it falls under an exception to the warrant requirement, it must be supported by probable cause.[31] Probable cause has its own definitional difficulties.[32] Generally, probable cause evaluations use a multi-factor, objective test: "[W]ould the facts available to the officer at the moment of the seizure or the search 'warrant a man of reasona-

---

23. *Id.* at 349–50.

24. *Id.* at 353.

25. *Id.* at 351.

26. *Id.* at 361 (Harlan, J., concurring).

27. *Id.* at 358–59 (majority opinion).

28. For information regarding exigent circumstances, see Michigan v. Fisher, 558 U.S. 45, 47 (2009) (emergency aid); Kentucky v. King, 563 U.S. 452, 460 (2011) (imminent destruction of evidence); United States v. Santana, 427 U.S. 38, 42–43 (1976) (hot pursuit); Carroll v. United States, 267 U.S. 132, 162 (1925) (border searches); Chimel v. California, 395 U.S. 752, 762–63 (1969) (protective searches).

29. 2 LAFAVE, *supra* note 12, § 4.1(a).

30. FED. R. CRIM. P. 41(e).

31. 2 LAFAVE, *supra* note 12, § 3.1(a).

32. *Id.* § 3.2(a). The Supreme Court held in *Illinois v. Gates* that "probable cause is a fluid concept − turning on the assessment of probabilities in particular factual contexts − not readily, or even usefully, reduced to a neat set of legal rules." Illinois v. Gates, 462 U.S. 213, 232 (1983).

ble caution in the belief' that the action taken was appropriate."[33] Determining whether sufficient evidence exists to support probable cause depends on a balancing test, weighing the invasiveness of the privacy interest against the nature of the immediacy at hand.[34]

B. Historic Surveillance Law Cases

As demonstrated in *Katz*, warrant and probable cause requirements in surveillance cases can raise interesting questions when criminals try to outpace law enforcement in the utilization of new technology.

The next major[35] development in surveillance law came in two beeper cases decided a year apart.[36] In *United States v. Knotts*, a beeper was hidden in a vat of chloroform that was used to locate a 3M employee who had stolen the chemical for purposes of manufacturing methamphetamine.[37] Law enforcement was able to closely follow the employee and locate the employee by using a monitoring device that captured the beeper's signal.[38] Once the signal was determined stationary at a secluded cabin in rural Wisconsin, police surveilled the cabin and secured a search warrant.[39] Law enforcement did not track the movement of the vat inside the cabin.[40] Later, evidence of the warrantless monitoring of the vat was admitted at trial.[41] In applying *Katz*, the Supreme Court held that that the governmental surveillance at issue amounted to the following of an automobile on public streets and highways, a place where the defendant had no reasonable expectation of privacy in his

33. Terry v. Ohio, 392 U.S. 1, 21–22 (1968) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)). *See also* 2 LAFAVE, *supra* note 12, § 3.2(a). In *Brinegar v. United States*, the Supreme Court held that probable cause determinations require "'less than evidence which would justify' . . . conviction," but "more than bare suspicion." Brinegar v. United States, 338 U.S. 160, 175 (1949) (quoting Locke v. United States, 11 U.S. (7 Cranch) 339, 348 (1813)).

34. 2 LAFAVE, *supra* note 12, §§ 3.2(a), (e).

35. In the 1970s, the Court issued equivocal rulings on the probable cause requirement within the domain of state surveillance law. *Compare* United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 323–24 (1972), *with* Smith v. Maryland, 442 U.S. 735, 745–46 (1979). Noticeably different in *Smith v. Maryland* was the operation authorized under the Pen Registers and Trap and Trace Statute, a legislative response to the Court's Fourth Amendment doctrine, which had made it increasingly difficult for law enforcement to surveil suspects by means of telephonic communication. *See Smith*, 442 U.S. at 737. In *Smith*, the court held that no search or seizure occurred. *Id.* at 745–46.

36. United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

37. *Knotts*, 460 U.S. at 277.

38. *Id.*

39. *Id.* at 278.

40. *Id.* at 285.

41. *Id.* at 279.

movements.[42] It further held that the defendant did not have a subjective expectation of privacy.[43] Since the search satisfied both prongs of the *Katz* test, the Court concluded there was no unreasonable search at issue.[44]

United States v. Karo presented the Supreme Court with another case involving law enforcement's use of a beeper hidden inside a container of ether.[45] The Court resolved the question left open by *Knotts*: whether the initial installation of a beeper in a drum of chemicals was a search when the drum was delivered to a buyer who had no knowledge of the hidden beeper.[46] Again applying *Katz*, the Court found that the recipient of the chemical drum had no subjective or reasonable expectation of privacy at the time of the installation of the beeper because he did not have possession of the drum at the time.[47] Further, whatever reasonable expectation of privacy the recipient had was diminished when he consented to the possibility of something – including a beeper – being inside the drum that was not supposed to be there upon transfer of possession.[48]

The Supreme Court emphasized that although the installation of the beeper did not constitute a search or seizure under *Katz*, it was still possible that an illegal search took place if the drum was monitored in a place the recipient did have an actual or reasonable expectation of privacy, such as his residence.[49] The Court further held that monitoring such devices required a warrant but left open the possibility of exceptions under exigent circumstances.[50]

Knotts and *Karo* represent the Supreme Court's approach to cases where law enforcement uses digital signals to locate suspects, an approach the Court used for the next quarter century.

---

42. *Id.* at 281.

43. *Id.* at 282.

44. *Id.* at 285. The Court's opinion, however, noticeably neglected the pressing issue of the warrantless installation of the beeper, which is noted in the concurrences of Justices Brennan, Blackmun, and Stevens. *Id.* at 285–86 (Brennan, J., concurring). This issue was resolved in *Karo*. United States v. Karo, 468 U.S. 705, 711 (1984).

45. *Karo*, 468 U.S. at 708.

46. *Id.* at 711.

47. *Id.*

48. *Id.*

49. The Court noted, "This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. . . . [W]e think that it does." *Id.* at 714.

50. *Id.* at 714–15, 718. Exigent-circumstances doctrine instructs "that emergency conditions may justify a warrantless search and seizure, especially when there is probable cause to believe that evidence will be removed or destroyed before a warrant can be obtained." *Exigent-circumstances doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014).

C. Modern Surveillance Statutory Scheme

Surveillance law in Missouri operates under the federal statutory scheme.[51] CSLI is accessed by law enforcement officers under a federal law, the Stored Communications Act (the "SCA").[52] The SCA requires companies, after receiving a proper application, to disclose the "contents" or "records" of electronic communications.[53] An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence . . . transmitted . . . by a wire, radio, electromagnetic, photoelectronic[,] or photooptical system."[54] Importantly, an electronic communication expressly does not include "any communication from a tracking device."[55]

The "contents" of an electronic communication are distinguishable from the "records" of an electronic communication.[56] "Contents" are defined as "any information concerning the substance, purport, or meaning" of an electronic communication, and contents are obtained under 18 U.S.C. §§ 2703(a) and (b).[57] The contents of a communication are more relevant to issues involving wiretapping than location tracking.[58] While not expressly defined under the SCA, "records" presumably extends to any information, retained by the cell service provider, that might not otherwise fall under the definition of "contents."[59] Records are obtained under 18 U.S.C. § 2703(c). The SCA's records provisions are relevant to the present discussion of CSLI because contents deal only with an electronic communication's meaning, and CSLI is merely data related to the electronic communication.[60]

There are five ways that electronic communication records, like CSLI, may be subject to compelled disclosure by and to law enforcement under the

---

51. While Missouri Revised Statutes sections 542.400–542.420 provide local law enforcement the ability to initiate a wiretap, state surveillance law is outdated by modern technology and limited to "wire communications." MO. REV. STAT. § 542.400 (Cum. Supp. 2013). "Wire communications" are defined as "any communication made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection." *Id.* § 542.400(12). While it is unclear whether "or other like connection" could be extended to mean cell towers, practically the statute is unused. In 2015, no Missouri court granted a surveillance order under the statute. WIRETAP REPORT 2015, *supra* note 2, at tbl.2.

52. The Stored Communications Act, 18 U.S.C.A. §§ 2701–2712 (West 2017).

53. The SCA incorporates the definitions under 18 U.S.C. § 2510. *Id.* § 2711(1). Further, 18 U.S.C. § 2703 requires electronic communication providers to turn over the "contents" of electronic communications under qualified circumstances. *Id.* § 2703(a).

54. *Id.* § 2510(12).

55. *Id.* § 2510(12)(C). A "tracking device" is defined in 18 U.S.C. § 3117(b).

56. The "contents" of an electronic communication are distinguished from "records" of an electronic communication in 18 U.S.C. § 2510(8).

57. § 2510(8). *See also id.* §§ 2703(a)–(b).

58. *See* CARR, BELLIA & CREUTZ, *supra* note 8, § 4:78.

59. *See* 18 U.S.C. § 2703(c).

60. *See* CARR, BELLIA & CREUTZ, *supra* note 8, § 4:78.

SCA, although only two are relevant for the purpose of this Note.[61] First, under § 2703(c)(1)(A), law enforcement may compel disclosure of electronic communication records when a warrant is obtained pursuant to federal or state rules of criminal procedure.[62] Second, under § 2703(c)(1)(B), law enforcement may compel disclosure under a court order.[63]

Warrant procedures for electronic communication records sought under § 2703(c)(1)(A) are no different than other warrants and thus are subject to the same constitutional requirements.[64] Probable cause must then be shown under § 2703(c)(1)(A).[65] If the warrant is sought before a federal court, the Federal Rules of Criminal Procedure expressly require a showing of probable cause to obtain a warrant "to search for and seize a person or property or to install and use a tracking device."[66] Under this rule, a tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[67]

However, if law enforcement does not have the necessary evidence to make the required probable cause showing, then it may obtain CSLI under the second method of § 2703(c)(1)(B), which has a lower standard.[68] Courts have held that this lower statutory standard is constitutionally permissible because the third-party disclosure doctrine applies to electronic communication records.[69] The third-party doctrine instructs that an individual does not have a reasonable expectation of privacy when that individual voluntarily

---

61. 18 U.S.C. § 2703(c).

62. *Id.* § 2703(c)(1)(A). If seeking a warrant in state court, then applicable state rules of criminal procedure govern, while if seeking a warrant before a federal court, the Federal Rules of Criminal Procedure operate. *Id.* §§ 2703(a)–(b). Since most warrants issued for required records disclosure under the SCA are sought in federal court, this Note primarily focuses on the Federal Rules of Criminal Procedure when relevant discussion arises. *See supra* note 2 and accompanying text.

63. 18 U.S.C. § 2703(c)(1)(B). Section 2703(c)(1) also provides that a record may be disclosed with the consent of the customer, for purposes of investigating a telemarketing scheme or when the information sought relates to billing information. *Id.* §§ 2703(c)(1)(C)–(E).

64. Section 2703(c)(1)(A) relies on "the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State Court, issued using State warrant procedures)." *Id.* § 2703(c)(1)(A). Courts have held that search and seizure provisions of the Federal Rules of Criminal Procedure "embod[y] standards which conform with the requirements of the Fourth Amendment." United States v. Haywood, 464 F.2d 756, 760 (D.C. Cir. 1972).

65. Federal Rule of Criminal Procedure 41 lays out the requirements of obtaining a warrant in federal courts. FED. R. CRIM. P. 41.

66. *Id.* at 41(d)(1).

67. The rule adopts the definition of a tracking device as found in 18 U.S.C. § 3117(b). FED. R. CRIM. P. 41(a)(2)(E).

68. *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) (holding "[t]his showing is lower than the probable cause standard required for a search warrant").

69. *See, e.g.*, United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016).

discloses information to third parties.[70] As a result of this exception to the constitutional probable cause requirement, under § 2703(c)(1)(B), a court order for disclosure of CSLI need only be supported by a standard of "specific and articulable facts" that show "reasonable grounds to believe" that the record is "relevant and material to an ongoing criminal investigation."[71] Importantly, a court order issued pursuant to § 2703(c)(1)(B) is expressly prohibited if it is in contravention of state law.[72]

CSLI is sometimes sought by law enforcement under joint authority of the Pen Registers[73] and Trap and Trace Devices[74] Statute, 18 U.S.C. §§ 3121–3127. The Pen Registers Statute was amended in 2001 by the USA PATRIOT Act to include "signaling information" as part of its definition of pen registers.[75] However, the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") provides that "call-identifying information" obtained under the Pen Registers Statute "shall not include any information that may disclose the physical location of the subscriber."[76] The legal standard under the Pen Registers Statute to obtain electronic communication records is even lower than the SCA's standard. Law enforcement requesting an order to establish a pen register or trap and trace device need only show the information "likely to be obtained . . . is relevant to an ongoing criminal investigation."[77] However, some courts have held that law enforcement seek-

---

70. The third-party disclosure doctrine is the view that a subject surrenders Fourth Amendment protections by revealing information to a third party. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

71. 18 U.S.C. § 2703(d) (2012).

72. *Id.* ("In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.").

73. A pen register is a device or process that "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," as long as the transmission does not include contents. *Id.* § 3127(3).

74. A trap and trace device "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(4).

75. *In re* Application of U.S. for Order, 497 F. Supp. 2d 301, 306 (D.P.R. 2007) (discussing the legislative history of the Communications Assistance for Law Enforcement Act and the Pen Registers Statute).

76. 47 U.S.C. § 1002(a)(2)(B) (2012).

77. 18 U.S.C. § 3123(a)(1). It is not immediately clear whether the standard laid out under the Pen Registers Statute is higher, lower, or the same as the standard under the SCA. The SCA requires the government to offer "specific and articulable facts" showing "reasonable grounds" that the information sought would be relevant to an ongoing criminal investigation. *Id.* § 2703(d). The Pen Registers Statute merely requires the government to certify that the information "likely to be obtained" is relevant. *Id.* § 3123(a)(1). The offering of "specific and articulable" facts requirement, which requires the government to detail its reasonable belief that the sought records

ing real-time CSLI cannot do so under CALEA – meaning CALEA can only be used to collect historic CSLI.[78]

Federal courts across the country have disagreed about the necessity of a warrant supported by probable cause for obtaining real-time CSLI. Some courts have held under the third-party disclosure doctrine that accessing real-time CSLI is not an unreasonable search under the Fourth Amendment because there is no objective expectation of privacy.[79] Other courts have held that the third-party disclosure doctrine does not apply because users do not voluntarily choose to share their location information with their service providers.[80] Courts in the First,[81] Second,[82] Fourth,[83] Fifth,[84] Sixth,[85] Seventh,[86]

---

will be relevant, is more strenuous than a mere government certification that the records are "likely" to be relevant. *Id.*

78. *See* United States v. Espudo, 954 F. Supp. 2d 1029, 1043 (S.D. Cal. 2013) (holding that a warrant sought under the hybrid standards of the SCA and Pen Registers Statute must be supported by probable cause because CALEA's legislative record does not support a hybrid theory interpretation of CALEA).

79. *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 136 (E.D.N.Y. 2013) (holding that cell phone users agree to be tracked because of the general public's awareness of geolocation tracking on cell phones, along with cell phone users' agreements with service providers and manufactures terms). *See also* United States v. Salas, No. 1496, 2013 WL 4459858, at *3 (E.D. Cal. Aug. 16, 2013) (holding that the third-party disclosure doctrine applies to CSLI).

80. *See* State v. Andrews, 134 A.3d 324, 351 (Md. Ct. Spec. App. 2016) (holding that the third-party disclosure doctrine is "ill suited to the digital age" and that cell phone users do not "voluntarily convey" information to service providers (quoting United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring))).

81. *See, e.g.*, *In re* Applications of U.S. for an Order Authorizing Continued Use of a Pen Register & Trap & Trace With Caller Identification Device, 530 F. Supp. 2d 367, 368–69 (D. Mass. 2007) (holding that the SCA was a sufficient standard for historic CSLI, but not for real-time or prospective data, which required a probable cause showing for required disclosure).

82. United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (holding that law enforcement needed an independent warrant supported by probable cause to use a cell-site simulator to obtain real-time CSLI).

83. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 541 (D. Md. 2011) (holding that probable cause must be shown to obtain a warrant for real-time CSLI because cell phone users keep their phone "on their person when conducting daily activities" and that cell phone users have a reasonable expectation of privacy in their movements).

84. *In re* Application of the U.S. for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Tel., 102 F. Supp. 3d 884, 895–96 (N.D. Miss. 2015) (noting the cautious approach of a U.S. Attorney who sought a warrant supported by probable cause "pending clarification regarding the applicable constitutional standards in the prospective cell phone data context").

85. United States v. Powell, 943 F. Supp. 2d 759, 778 (E.D. Mich. 2013).

86. *In re* U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004, 2006 WL 2871743, at *5 (E.D. Wis. Oct. 6, 2006) (holding

and Ninth Circuits have required a warrant issued on probable cause before police can collect real-time CSLI.[87] But courts within the Tenth[88] and Eleventh[89] Circuits only require the fulfillment of one of the lesser standards articulated in the SCA or Pen Register Statutes. Circuit courts that have addressed the issue of CSLI include the Fourth,[90] Sixth,[91] and Eleventh[92] Circuits. The Eighth Circuit has not addressed the issue of Fourth Amendment searches and real-time CSLI under the SCA.[93]

Despite the discordant body of case law surrounding the issue of CSLI, recent developments at the Supreme Court and corresponding reactions by state legislatures appear to be trending in favor of individual digital privacy interests.

III. RECENT DEVELOPMENTS

Part A of this section first discusses recent developments in case law that have potential bearing on the issue of Missouri surveillance law and electronic communications and data. Part B of this section then discusses Missouri's recent constitutional amendment to article I, section 15.

A. Relevant Case Law Developments

Whether the monitoring of real-time CSLI is a search under the Fourth Amendment is an open question under Supreme Court jurisprudence. Relevant developments involve the Supreme Court's recent consideration of the nature of Global Positioning System ("GPS") information,[94] as well as a law enforcement search of a cell phone incident to arrest.[95]

---

that the lesser standards of the SCA and Pen Registers Statute were insufficient to support a warrant seeking to obtain CSLI).

87. *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1039 (N.D. Cal. 2015) (holding that the third-party disclosure doctrine did not apply because cell phone users do not generally consent through privacy policies to the warrantless acquisition of CSLI).

88. United States v. Takai, 943 F. Supp. 2d 1315, 1323 (D. Utah 2013) (holding that warrant exceptions applied in emergency circumstances).

89. United States v. Booker, No. 1:11–CR–255–1–TWT, 2013 WL 2903562, at *7 (N.D. Ga. June 13, 2013).

90. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016).

91. United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

92. Davis v. United States, 785 F.3d 498, 511 (11th Cir. 2015).

93. The Eighth Circuit has analyzed emails under the SCA. *See* United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (holding that a search and seizure of emails conducted by technicians as directed by law enforcement was not a violation of the Fourth Amendment); Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 842 (8th Cir. 2015) (holding that sent and draft emails were not "stored" within the meaning of the SCA).

94. United States v. Jones, 565 U.S. 400, 402 (2012).

95. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

In *United States v. Jones*, the Supreme Court returned to issues relating to law enforcement's use of tracking devices.[96] In *Jones*, the Court held that a warrantless attachment of a GPS tracking device to a vehicle was an unreasonable search under the Fourth Amendment.[97] The investigating officers obtained a warrant authorizing the use of an electronic tracking device on the suspect's wife's Jeep.[98] However, the officers failed to install the device during the period authorized by the warrant.[99] Undeterred, law enforcement installed the GPS device a day after the period lapsed.[100] Law enforcement then tracked the suspect's movement for the next twenty-eight days.[101]

Writing for the majority, Justice Scalia resurrected the trespassory test often used by the Supreme Court prior to *Katz*. Scalia argued that the *Katz* test was an addition to – not a substitute for – the common law trespassory test.[102] Scalia reasoned that the *Katz* test would still apply in situations involving "merely the transmission of electronic signals without trespass."[103]

In concurrence, Justice Sotomayor raised concerns about the application of the third-party disclosure doctrine in the context of surveillance and electronic communications.[104] Also writing in concurrence, Justice Alito argued that the trespassory test presented numerous problems[105] in a digital age.[106] He further argued that even the *Katz* test might be inadequate to address privacy concerns arising from the monitoring of electronic devices.[107] Finally,

---

96. *Jones*, 565 U.S. at 404.

97. *Id.*

98. *Id.* at 402–03.

99. *Id.*

100. *Id.*

101. *Id.* at 403.

102. *Id.* at 406–07. Scalia read *Knotts* and *Karo* to support this argument because neither case questioned the unauthorized installation of a beeper by law enforcement (*Knotts*) or a third party (*Karo*). *Id.* at 409.

103. *Id.* at 411.

104. *Id.* at 416 (Sotomayor, J., concurring).

105. First, the majority's disregard for the use of GPS for purposes of long-term tracking, instead emphasizing the "relatively minor" attachment of the GPS to a vehicle. *Id.* at 424–25 (Alito, J., concurring). Second, the majority's approach leads to "incongruous results," in that if police attach a GPS to a vehicle, then the Fourth Amendment applies, but if the police follow the vehicle "for a much longer period using unmarked cars and aerial assistance," then there are no Fourth Amendment issues. *Id.* at 425. Third, under the majority's approach, the "coverage of the Fourth Amendment may vary from state to state" based upon the state's approach to community property. *Id.* at 425–26. Some "non-community-property" states would interpret the registration of the Jeep in the wife's name as presumptive evidence that the wife was the sole owner. *Id.* at 426. Finally, the majority's approach fails to account for cases of involuntary transmission of electronic signaling, such as tracking a vehicle by activating stolen vehicle detection systems or potentially CSLI, because no physical touching of the property has occurred. *Id.*

106. *Id.* at 418.

107. *Id.* at 426–27.

he suggested that the most effective way to check the surveillance power of the government was through legislation.[108]

Two years later, in *Riley v. California*, the Supreme Court unanimously rejected the incident to arrest warrant exception for searches of data on cell phones.[109] Writing for the majority, Chief Justice Roberts emphasized the unique nature of the cell phone, based on its enormous capacity to store information and the nature of the information stored on a cell phone.[110] Roberts outlined the intimate nature of stored cell phone data, potentially ranging from sexual preferences to personal concerns about one's health.[111] Importantly, Roberts saw that the search of stored data on a cell phone could be far more invasive than the search of a home.[112] Roberts echoed Sotomayor's concern in *United States v. Jones*, writing that cell phone location information is standard on most modern phones "and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[113] The Supreme Court's ruling in *Riley* recognized a long-vocalized concern regarding the nature of privacy in a digital age.

B. Article I, Section 15

In 2014, Missouri amended article I, section 15 of the Missouri Constitution to read,

> That the people shall be secure in their persons, papers, homes, effects, and *electronic communications and data*, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, or *access electronic data or communication*, shall issue without describing the place to be searched, or the person or thing to be seized, or the *data or communication* to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation.[114]

The amendment came before the public for a vote upon the legislature's initiative.[115] Upon first introduction, the legislature's bill summary read that prior to issuance, a warrant "must describe the data or communication to be

108. *Id.* at 429–30.
109. Riley v. California, 134 S. Ct. 2473, 2485 (2014).
110. *Id.* at 2489–90.
111. *Id.*
112. *Id.* at 2490–91.
113. *Id.* at 2490.
114. MO. CONST. art. I, § 15 (emphases added).
115. S.J. Res. 27, 97th Gen. Assemb., 2d Reg. Sess. (Mo. 2014).

accessed and be supported by probable cause."[116] The language of the proposed amendment remained unchanged throughout the legislative process.[117]

By passing the amendment, Missouri voters became the first state to enshrine protections for electronic communication and data in their constitution.[118] In a media report following the passage of the amendment, the bill's original sponsor, Senator Robert Schaaf, noted that the amendment's legal impact would "take time to sort out," but the legislative intent was to afford electronic communications and data the same protections provided to other enumerations of "person, paper, home, and effects," as provided under article I, section 15.[119]

While the Supreme Court of Missouri has yet to substantially address the amendment to article I, section 15, the Missouri Court of Appeals, Western District, has discussed the implications of the new "electronic communications and data" provision in a context unrelated to CSLI.[120] In *State ex rel. Koster v. Charter Communications, Inc.*, the Western District interpreted the recent amendment as having no effect on current search and seizure law.[121] The court held that "article I, section 15, even as amended, is not currently measurably more restrictive on the government than is the Fourth Amendment."[122] The Supreme Court of Missouri has traditionally read article I, section 15 to be "coextensive" with the Fourth Amendment.[123]

However, these interpretations of article I, section 15 do not negate the clear requirement of a warrant supported by probable cause when law enforcement seeks electronic communications and data. This requirement of probable cause extends to disclosure requests sought under § 2703(c) of the SCA for purposes of monitoring real-time CSLI, despite the SCA's articulated standard of "specific and articulable facts" for the reasons set forth in the next section.

---

116. *Id.*

117. *Compare* S.J. Res. 27, 97th Gen. Assemb., 2d Reg. Sess. (Mo. 2014) (prefiled Dec. 1, 2013, version), *with* S.J. Res. 27, 97th Gen. Assemb., 2d Reg. Sess. (Mo. 2014) (enacted).

118. Becca Stanek, *Missouri Passes Constitutional Amendment to Protect Electronic Privacy*, TIME (Aug. 6, 2014), http://time.com/3087608/missouri-electronic-privacy-amendment/. A number of other states have since implemented statutory measures affording similar protections to electronic communications and data. *State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

119. Stanek, *supra* note 118.

120. State *ex rel.* Koster v. Charter Commc'ns, Inc., 461 S.W.3d 851, 857–58 (Mo. Ct. App. 2015).

121. *Id.* at 858. The Western District wrongly interpreted the effect of the amendment on article I, section 15 by neglecting long-practiced rules of constitutional construction. *See* Pestka v. State, 493 S.W.3d 405, 408–09 (Mo. 2016) (en banc). *See also infra* Part IV.A.

122. *Charter*, 461 S.W.3d at 858.

123. State v. Hosier, 454 S.W.3d 883, 892 n.6 (Mo. 2015) (en banc).

IV. DISCUSSION

Article I, section 15 requires a warrant supported by probable cause for purposes of monitoring real-time CSLI because the provision is broader in its scope of protections than the Fourth Amendment. Article I, section 15 is broader in its scope of protections than the Fourth Amendment both on its face and because of its legislative purpose. The legislative purpose of the amendment defeats the warrant exception for real-time CSLI under the third-party disclosure doctrine because CSLI is qualitatively a different kind of record than what is traditionally treated as a record under the doctrine. Moreover, probable cause must support a warrant for real-time CSLI because the SCA's standard is ill-fitting in the circumstances that real-time CSLI is often sought.

A. Article I, Section 15 Is Broader on Its Face and Through Its Legislative Purpose Than the Fourth Amendment

The plain text of article I, section 15 includes a specific enumeration for "electronic communications and data," language that is absent from the Fourth Amendment.[124] In Missouri, constitutional provisions "are subject to the same rules of construction as other laws, except that constitutional provisions are given a broader construction due to their more permanent character."[125] Additionally, it must be assumed that every word "contained in a constitutional provision has effect, meaning, and is not mere surplusage."[126] Generally, words are interpreted to "give effect to their plain . . . meaning."[127] One of the accepted canons of statutory construction is an examination of the legislative development of the provision and related statutes.[128]

Article I, section 15's language, "electronic communications and data," cannot be read to be "mere surplusage" because every word "contained in a constitutional provision" is given meaning and effect.[129] To read article I, section 15 to be coextensive with the Fourth Amendment after its 2014 amendment, however, does render "electronic communications and data" mere surplusage. Article I, section 15 was read coextensively with the Fourth Amendment prior to article I, section 15's amendment.[130] So Missouri courts

124. *Compare* U.S. CONST. amend. IV, *with* MO. CONST. art. I, § 15.

125. *Pestka*, 493 S.W.3d at 408–09 (quoting Neske v. City of St. Louis, 218 S.W.3d 417, 421 (Mo. 2007) (en banc)).

126. *Id.* at 409 (quoting State v. Honeycutt, 421 S.W.3d 410, 415 (Mo. 2013) (en banc)).

127. *Id.* (quoting Wright-Jones v. Nasheed, 368 S.W.3d 157, 159 (Mo. 2012) (en banc)).

128. *Id.*

129. *Id.* (quoting *Honeycutt*, 421 S.W.3d at 415).

130. *See* State v. Lovelady, 432 S.W.3d 187, 190 (Mo. 2014) (en banc); State v. Grayson, 336 S.W.3d 138, 151 n.4 (Mo. 2011) (en banc). *Compare* MO. CONST. art. I, § 15 (current), *with* MO. CONST. art. I, § 15 (1945).

understood the Fourth Amendment to either (1) not protect or (2) already protect "electronic communications and data." In either case, a post-amendment coextensive reading of article I, section 15 would render "electronic communications and data" surplusage. Such a reading is to be avoided under Missouri's rules of construction.[131] Therefore, article I, section 15 must be broader in its scope of protections than the Fourth Amendment because Missouri changed its search and seizure language, which had previously mirrored the Fourth Amendment, to include a specific enumeration for "electronic communications and data," and this change is to be given meaning and effect.[132]

This does not resolve, however, what the meaning and effect of those added protections are under article I, section 15. To determine this, under Missouri's rules of construction, "electronic communications and data" must be interpreted to give effect to the plain meaning, alongside an examination of the legislative development of the provision and related statutes.[133]

"Electronic communications and data" is a broad category, the definition of which Missouri courts have not limited; nor has the legislature defined it.[134] In the case of article I, section 15, the development of the ballot initiative through the General Assembly offers little insight into the legislative meaning of "electronic communications and data" because the provision was adopted without substantial alteration.[135] No other relevant state statute em-

131. Prior to the passage of the 2014 amendment to article I, section 15, the court held the provision to be "coextensive with the Fourth Amendment; consequently 'the same analysis applies under both provisions.'" *Lovelady*, 432 S.W.3d at 190 (quoting *Grayson*, 336 S.W.3d at 143 n.2). In 2015, the court discussed the issue of real-time CSLI and probable cause requirements. State v. Hosier, 454 S.W.3d 883, 892 (Mo. 2015) (en banc). The discussion did not produce a relevant holding because the events of the case took place prior to the amendment; however, it did indicate that the court is well aware of the unresolved question. *Id.* The court discussed "[t]he issue of whether police must make a probable cause showing in order to obtain real-time cell phone location data" as one "frequently challenged," but "[n]o Missouri state court has ruled on [the] issue." *Id.*

132. *See Honeycutt*, 421 S.W.3d at 414–15 (holding that the court's "primary goal in interpreting Missouri's constitution is to 'ascribe to the words of a constitutional provision the meaning that the people understood them to have when the provision was adopted'" (quoting Farmer v. Kinder, 89 S.W.3d 447, 452 (Mo. 2002) (en banc))). It follows that if prior to its amendment, article I, section 15 and the Fourth Amendment were coextensive, then following its amendment, article I, section 15 extends beyond the protections of the Fourth Amendment. The extent of these protections depends on what "meaning and intent" are given to "electronic communications and data." *Id.*

133. *Pestka*, 493 S.W.3d at 409.

134. *Hosier*, 454 S.W.3d at 892 n.6.

135. *Compare* S.J. Res. 27, 97th Gen. Assemb., 2d Reg. Sess. (Mo. 2014) (prefiled Dec. 1, 2013, version), *with* S.J. Res. 27, 97th Gen. Assemb., 2d Reg. Sess. (Mo. 2014) (enacted).

ploys the phrase "electronic communications and data."[136] With little help forthcoming from Missouri's scant legislative history, it is helpful to look to federal statutes and other jurisdictions to determine what the legislature was intending to do.

Under 18 U.S.C. § 2510, which the SCA relies on for definitions, an "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, [or] electromagnetic . . . that affects interstate or foreign commerce[,] . . . [except] any communication from a tracking device."[137] It is possible to conclude that Missouri's legislature, in contemplating an amendment to its constitutional search and seizure provision, would have considered the federal scheme governing the search and seizure of electronic communications. Further, it is reasonable that this definition was the one intended by the legislature when it proposed amending article I, section 15 to include protections for "electronic communication and data" because both provisions' use of the term of art is in the context of search and seizure by a governmental entity.

A look at other jurisdictions further supports an adoption of 18 U.S.C. § 2510's definition of "electronic communication." While Missouri was the first state to enshrine protections for digital privacy in its constitution, it was not alone in taking up Justice Alito's suggestion for legislative action mentioned in his concurrence in *United States v. Jones*.[138] Several other states have passed legislation affording protections to digital privacy.[139] Two statutes are noteworthy for the current discussion.

First, Maine enacted an electronic privacy statute in 2014.[140] The statute imposes a warrant requirement, supported by probable cause,[141] on law enforcement when it is seeking to obtain location information, such as CSLI, of

136. An unrelated state regulation uses the phrase "electronic communications and data" in the context of defining a "statistical agent" as part of Missouri's Life Insurance and Annuity Standards regulations. MO. CODE REGS. ANN. tit. 20, § 400-1.170(1)(C) (2017).

137. 18 U.S.C. § 2510(12) (2012). A tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *Id.* § 3117(b).

138. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

139. *See* N.H. REV. STAT. ANN. § 644.21 (2017); TEX. CODE CRIM. PROC. ANN. art. 18.02 (West 2017); UTAH CODE ANN. § 63D-2-103 (West 2017); MINN. STAT. ANN. § 13.15 (West 2017); CAL. GOV'T CODE § 11019.9 (West 2017). This list is not exhaustive.

140. Hanni Fakhoury, *Why Wait for Congress? States Passing Electronic Privacy Legislations*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS (June 3, 2013), https://www.eff.org/deeplinks/2013/05/why-wait-congress-states-passing-electronic-privacy-legislation. *See also* 16 ME. REV. STAT. ANN. tit. 16, § 648 (2017).

141. 16 ME. REV. STAT. ANN. tit. 16, § 648.

an electronic device.[142] Second, California enacted its Electronic Communications Privacy Act, which likewise requires a showing of probable cause[143] upon issuance of a warrant to obtain electronic information.[144] Under California's law, electronic information is defined as a class of data resulting from an electronic communication.[145] California's definition of electronic communication tracks the language of 18 U.S.C. § 2510.[146]

In proposing a referendum to alter article I, section 15, Missouri likely shared the same understanding as California as to the meaning of "electronic communications" and its "data," as both legislatures reacted to the same digital privacy concerns raised by *United States v. Jones*.[147] Further, real-time CSLI should be held within the meaning of "communications data" because other similarly reacting legislatures, like Maine, specifically contemplated it to be a type of data identified as a concern by the *Jones* concurrences.[148] Finally, the canons of construction under *Pestka* require a broad construction of article I, section 15 because of the "permanent character of constitutional provisions," resulting in the incorporation of CSLI within the meaning of communication data.[149]

A broad construction of "electronic communications and data" does not, however, necessarily overcome application of traditional constitutional exceptions to the warrant requirement for searches and seizures – such as the third-party disclosure doctrine. To support the claim that a warrant supported by probable cause is required to obtain real-time CSLI, it must be shown that the third-party disclosure doctrine does not apply.

---

142. Maine's statute was enacted the same year article I, section 15 of the Missouri Constitution was amended. *See* 16 ME. REV. STAT. ANN. tit. 16, § 648; *see also* MO. CONST. art I, § 15.

143. CAL. PENAL CODE § 1546.1(d)(2) (West 2017).

144. *Id.*

145. *Id.* §§ 1546.1(c)–(d), (h).

146. *Compare id.* §§ 1546.1(c)–(d), (h), *with* 18 U.S.C. § 2510(12) (2012).

147. Indeed, legislators who advocated for the referendum's passage expressly noted that the amendment would protect "private communications and data from being sent[or] disclosed . . . to some other third party." *See* Cody Newill, *Voter Guide to Missouri Constitutional Amendment 9*, KCUR 89.3 (July 28, 2014), http://kcur.org/post/voter-guide-missouri-constitutional-amendment-9. Sotomayor and Alito's concerns about the third-party disclosure doctrine drove their discussion in *United States v. Jones*. *See supra* Part III.A.

148. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). *See also id.* at 418–31 (Alito, J., concurring).

149. *See* Pestka v. State, 493 S.W.3d 405, 408–09 (Mo. 2016) (en banc).

B. The Third-Party Disclosure Doctrine Does Not Apply to Real-Time CSLI Under Article I, Section 15

The third-party disclosure doctrine is often used by law enforcement to obtain digital records held by cell phone companies.[150] It has historically applied in two types of circumstances: those involving undercover informants and those involving third-party business records.[151] A business record is "[a] report, memorandum, or other record made usually in the course of business."[152] The business records class of circumstances is relevant in the CSLI context.

Because real-time CSLI is qualitatively different than other business records accessible under the third-party disclosure doctrine, the doctrine should not apply to real-time CSLI under article I, section 15.[153] This qualitative difference was noted by Justices Alito and Sotomayor in *Jones*, along with Chief Justice Roberts in *Riley*.[154]

In *Riley v. California*, the Supreme Court recognized for the first time the problems posed by allowing law enforcement to access cell phone data and records, including locational data.[155] The Court outlined three distinguishing features that inform how courts analyze privacy issues relating to cell phones and records access.[156] First, cell phones have many distinct types of information, including addresses, videos, and bank statements, that reveal more than any isolated record.[157] Second, cell phones have a large capacity to store this varied information.[158] Third, cell phones are more pervasive than any other type of device that stores records.[159] The Court's skepticism about giving law enforcement easy access to cell phone data and records resulted in a ruling that required law enforcement to obtain a warrant to search a cell phone because of the vast and potentially intimate nature of personal information contained on cell phones.[160] A search of a cell phone "bears little resemblance" to other types of physical searches, including those of homes, because cell phone data may be used to "reconstruct someone's specific

150. Kerr, *supra* note 70, at 563.

151. *Id.* at 566.

152. *Business record*, BLACK'S LAW DICTIONARY (10th ed. 2014).

153. Stanek, *supra* note 118.

154. In *Jones*, Justice Sotomayor notes this tension between the third-party doctrine and digital privacy issues. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring). *See also* Riley v. California, 134 S. Ct. 2473, 2490 (2014).

155. *Riley*, 134 S. Ct. at 2485.

156. *Id.* at 2489.

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.* at 2485.

movements down to the minute, not only around town but also within a particular building."[161]

The addition of "electronic communications and data" to article I, section 15 may be interpreted as a response to the Court's turn in *Jones*. Scalia's application of the trespassory test in *Jones* could be viewed as narrowing the Fourth Amendment protections to items enumerated in the Fourth Amendment, including "persons, houses, papers, and effects." Writing for the majority, Justice Scalia argued that the privacy interest at issue during a search or seizure was to be narrowly analyzed as a property interest in the thing being searched.[162] Scalia concluded that an unreasonable search had occurred during the GPS monitoring only because the GPS was placed on the defendant's wife's property, her Jeep.[163] This interference with the private property interest meant the search failed the trespassory test.

But it is more likely that *Jones* will be remembered for its concurrences, where Justices Alito and Sotomayor wrote separately to express concern about the trespassory approach in the case of CSLI.[164] Justice Sotomayor strongly advocated the reconsideration of the third-party disclosure doctrine, writing that it "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[165]

Justice Alito noted that Scalia's trespassory approach is problematic in the case of surreptitiously obtained cell phone data because there is no physical touching to satisfy trespass requirements, and the property interest is tenuous.[166] Instead, Alito suggested that Congress was best fitted to resolve the Fourth Amendment problems presented by the confluence of new technologies, like smart phones.[167] Seemingly on cue, Missouri reacted with its amendment to article I, section 15. As a response to *Jones*, Missouri's amendment to article I, section 15 expresses a clear and unambiguous policy to protect the ever-increasingly intimate nature of cell phone data and records. Modern cell phones provide stringent encryption capabilities and utilize biometric software to protect the privacy of their owners. These precautions indicate that both cell phone companies and users have a strong expectation of privacy regarding data associated with cell phones.

Beyond the mere policy endorsement of Missourians, real-time CSLI is a qualitatively different type of record than what is often obtained under the

161. *Id.* at 2490. The Court went on: "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone . . . contains a broad array of private information never found in a home in any form – unless the phone is." *Id.* at 2491.

162. United States v. Jones, 565 U.S. 400, 405 (2012).

163. *Id.* at 404–05.

164. *Id.* at 424–27 (Alito, J., concurring); *see also id.* at 414 (Sotomayor, J., concurring).

165. *Id.* at 417 (Sotomayor, J., concurring).

166. *See supra* note 105 and accompanying text.

167. *Jones*, 565 U.S. at 429–30 (Alito, J., concurring).

third-party disclosure doctrine because cell phone users do not voluntarily disclose CSLI in the same way that other business records are voluntarily disclosed.[168] The differences between voluntary disclosure of CSLI and other business records accessed under the third-party disclosure doctrine are that (1) cell phones are nearly ubiquitous and (2) carried on a person nearly everywhere he or she goes, including inside the constitutionally protected area of the home. This ubiquity results in real-time CSLI functioning more like a tracking device than a business record. Cell phones emit signals by merely being turned on. The voluntary act of turning on a phone and carrying it on one's person seems quite different than signing a business record, such as a bank document.[169]

Federal and state warrant procedures emphatically require a showing of probable cause to use a tracking device in criminal investigations.[170] So if CSLI functions like a tracking device, then probable cause should be needed to support a warrant that seeks to obtain real-time CSLI.

Under this view, real-time CSLI may not be sought under the SCA's court order provision, which only requires a showing of "specific and articulable facts" that the resulting evidence is likely to be relevant to an ongoing criminal investigation.[171] The court order provision implicitly reads real-time CSLI to be like other business records excepted by the third-party disclosure doctrine. But since real-time CSLI is more like a tracking device than a business record, this method of going around the probable cause requirement should be foreclosed to law enforcement.

This view is further buttressed when considering that the SCA expressly states that its lesser standard does not apply if in contravention to state law.[172] Since Missouri's article I, section 15, a state law, encompasses real-time CSLI, probable cause should be shown to obtain real-time CSLI.

---

168. *See, e.g.*, *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 538 n.6 (D. Md. 2011).

169. The inadequacy of the third-party disclosure doctrine is further highlighted when considering the emergence of the doctrine: "The third party and public exposure doctrines emerged at a time when modern surveillance capabilities were beyond imagination. Today, these previously unimaginable technologies are not merely law enforcement tools; they are essential parts of our daily lives." Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 301 (2015).

170. FED. R. CRIM. P. 41(d)(1).

171. *See* 18 U.S.C. § 2703(c) (2012).

172. The statute reads: "In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State." *Id.* § 2703(d).

C. The SCA's "Specific and Articulable Facts" Standard Is Ill-Fitting for CSLI Obtainment

Prior to Missouri's amendment to its constitutional search and seizure provision, law enforcement was permitted under the SCA's § 2703(c) to obtain real-time CSLI on issuance of a warrant supported by the lesser standard of "specific and articulable facts" that the communication was relevant to an ongoing criminal investigation. This standard was ill-fitting to CSLI from the beginning of the SCA, and article I, section 15's realignment to the probable cause standard fits the surveillance tactic with an appropriate standard.

The SCA's "specific and articulable facts" standard was not invented by Congress.[173] Instead, the language originated in the Supreme Court and has subsequently appeared in over seventy of their opinions.[174] Relevant cases analyze the "reasonable suspicion" law enforcement must have to authorize a limited search of a person or location.[175] The showing of "specific and articulable facts" is typically made to justify a search after the fact.[176] This alone makes the standard ill-fitting to real-time CSLI, which seeks to obtain future information rather than to justify a prior search. If that were not enough, many of the cases allowing a search under a "specific and articulable facts" standard only permitted the search because of the imminent potential danger presented to law enforcement or because the search was conducted during the commission of an ongoing crime.[177] Rarely is there an imminent potential danger presented to law enforcement during a search of real-time CSLI, and should such a case exist, the exigent-circumstances doctrine would apply. Likewise, the exigent-circumstances doctrine would seem to apply if law enforcement knew that a cell phone owner was committing a felony. But, in such a case, law enforcement would have to possess an inhuman clairvoyance to predict crimes before they happen.

---

173. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 7:51.20 (2016).

174. *Id.*

175. *Id. See* Maryland v. Buie, 494 U.S. 325, 334 (1990) (holding that protective sweep of home was authorized when police did not have probable cause or a warrant but could demonstrate a reasonable belief of specific and articulable facts that a potential danger was posed to the police officers at the arresting scene). *See also* Terry v. Ohio, 392 U.S. 1, 24 (1968) (holding that a pat down search was reasonable when law enforcement had a justified belief based on suspicious behavior that the arrested individual may pose a threat of danger).

176. FISHMAN & MCKENNA, *supra* note 173.

177. *See Buie*, 494 U.S. at 334 (holding that the Fourth Amendment permits law enforcement to conduct a protective sweep to search for an individual posing a danger to law enforcement officers or others); United States v. Hensley, 469 U.S. 221, 227–29 (1985) (holding that law enforcement may conduct a *Terry* stop when law enforcement believes that the person subject to the stop is involved in or is wanted in connection with a completed felony).

For these reasons, probable cause is the appropriate standard for a surveillance tactic like monitoring real-time CSLI. With the amendment to article I, section 15, probable cause must now support a warrant to obtain real-time CSLI.

V. CONCLUSION

Legislatures across the country have responded vigorously to rising concerns over digital privacy and locational data. Many states have enacted statutes that extend more protections for digital privacy. In Missouri, these protections have extended to the search of real-time CSLI. With its amendment to article I, section 15, Missouri has abrogated the application of the third-party disclosure doctrine to real-time CSLI because CSLI is unlike typical records excepted from probable cause requirements under the doctrine. Law enforcement that wishes to obtain real-time CSLI must now do so under a warrant supported by probable cause. Not doing so will result in an unreasonable search, which risks exclusion at trial of any obtained evidence during the search.